RR RUEHAG RUEHAO RUEHAP RUEHAT RUEHBC RUEHBI RUEHBL RUEHBZ RUEHCD
RUEHCHI RUEHCI RUEHCN RUEHDA RUEHDE RUEHDF RUEHDT RUEHDU RUEHED RUEHEL
RUEHFK RUEHFL RUEHGA RUEHGD RUEHGH RUEHGI RUEHGR RUEHHA RUEHHM RUEHHO
RUEHHT RUEHIHL RUEHIK RUEHJO RUEHJS RUEHKN RUEHKR RUEHKSO RUEHKUK
RUEHKW RUEHLA RUEHLH RUEHLN RUEHLZ RUEHMA RUEHMC RUEHMJ RUEHMR RUEHMRE
RUEHMT RUEHNAG RUEHNG RUEHNH RUEHNL RUEHNP RUEHNZ RUEHPA RUEHPB RUEHPD
RUEHPOD RUEHPT RUEHPW RUEHQU RUEHRD RUEHRG RUEHRN RUEHROV RUEHRS
RUEHTM RUEHTRO RUEHVC RUEHVK RUEHYG
DE RUEHC #2582/01 2981656
ZNR UUUUU ZZH

R 221850Z OCT 08
FM SECSTATE WASHDC
TO ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE
RUEHTRO/AMEMBASSY TRIPOLI 3637/3638

UNCLAS SECTION 01 OF 02 STATE 112582

C O R R E C T E D C O P Y (REMOVING FOR IMO)

INFORM CONSULS

E.O. 12958: N/A
TAGS: AINF AMGT APER ASEC CMGT
SUBJECT: RULES OF BEHAVIOR FOR PROTECTING PERSONALLY IDENTIFIABLE INFORMATION

BEGIN SUMMARY: The Privacy Act requires that rules of behavior, including penalties for noncompliance, exist for employees (including contract employees) involved in the design, development, operation, or maintenance of systems records covered by the Act. OMB Memorandum M-07-16 dated May 22, 2007, titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)," requires agencies to ensure that "managers, supervisors, and employees be informed and trained regarding their respective responsibilities relative to safeguarding personally identifiable information and the consequences and accountability for violation of these responsibilities." PII refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. END SUMMARY

¶1. The Department has long been concerned with protecting individuals' personal information. This concern has been heightened in recent years by the increasing mobility of information by electronic means and high visibility breaches of personal information in both paper and electronic formats. We all have an obligation to make certain that personally identifiable information is protected through appropriate safeguards to ensure security, privacy and integrity.

¶2. PII refers to information which can be used to "distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

¶3. Following are privacy rules of behavior applicable to Department of State records, regardless of format, that include PII. All employees and contractors with access to PII in the performance of their official duties are required to comply with these rules. These rules should be applied with due regard for the content and/or context of the underlying information. While all PII warrants appropriate protection, a list of employees' Social Security numbers or personal medical information is certainly more sensitive than a single address or telephone number of a professional associate.

Do not inspect, search, or browse PII records in files or databases unless you are authorized to do so in the performance of your official duties and have a need to do so

to accomplish your assigned work.

Do not disclose PII to others, including other authorized users, in any manner (electronically, verbally, etc.) unless there is a need to do so in the performance of your official duties.

Take special precautions to protect your computer passwords and other credentials that give access to PII.

Use a complex password.

Do not reveal your passwords to others.

Do not use your password when/where someone might see and remember it.

Do not store PII in shared electronic folders or shared network files that can be accessed by individuals without a "need to know."

Only alter or delete PII as may be necessary as part of an official duty.

Do not remove PII from your Department of State workplace unless it is for an approved purpose such as performing your duties under an official telecommuting agreement, to support the needs of temporary duty travel, or other such necessary offsite situations. Any PII removed should be the minimum amount reasonably necessary to accomplish your work and be returned promptly. Consult a supervisor before removing any significant number of PII records.

Storing PII on any computing device not owned by the government is prohibited.

Storing PII on mobile government furnished equipment is permitted if the data is encrypted in an approved way.

Use OpenNet Everywhere ("ONE") when feasible for the secure remote transmission of PII to the Department's sensitive but unclassified network (OpenNet) from any internet-connected computer that meets the system requirements for ONE.

Any unencrypted electronic transmission of PII over the internet must be done with due recognition of its sensitivity and a consideration of security risk. The greater the sensitivity and/or amount of PII to be transmitted, the more appropriate it may be to employ a secure alternative method of transmission (e.g., ONE, or a password-protected or encrypted document in which the password is conveyed separately). For further guidance refer to 12 FAM 544.3 and the A Bureau Privacy website.

Protect access to all media on which you process PII about others.

Lock your workstation before leaving your desk.

Limit physical access to workstations and documents.

In your office, or while using a portable device in a public place such as an airport, secure or shield your computer screen from view, reposition the computer display, or attach a privacy screen, when appropriate.

At the office, store hard copies containing PII in locked containers or rooms.

Safeguard hard copies of PII taken to your home, hotels, or other such locations outside your office. For example, store PII in a locked briefcase or desk in a home office. PII should be secured in hotel rooms (e.g., lock in room safe) and should not be left unattended in public spaces. For further guidance refer to 12 FAM 682.2-5.

Protect against eavesdropping on telephones or other conversations that involve other employees' or customers' PII.

¶4. All employees and contractors are held responsible for complying with these requirements. Failure by employees to comply with these rules may result in discipline, up to and including removal, or other action as appropriate. Failure by a contract employee to comply with these rules may result in permanent removal and/or other contractual sanctions. Also, please be aware that the Privacy Act provides for criminal penalties for government employees and contract employees in some circumstances for willful disclosure of Privacy Act protected information.

¶5. This rule set will be posted on the Bureau of Administration, Information Sharing Services, Information Programs and Services "Privacy Matters" and may be updated from time to time, as new rules are mandated externally or are needed to deal with new risks. These rules also will be incorporated into 5 FAM 460. Employees and contractors are urged to review this website and/or the appropriate FAM sections at the beginning of each quarter (or when notified to do so on an event-driven basis) to re-familiarize themselves with these rules and to check for additional requirements.

¶6. Questions should be addressed to the e-mail addresses listed on the A Bureau Privacy Website,"Privacy Matters," website.

¶7. Minimize considered.
RICE